EUROPEAN VIEW (2016) 15:133–144
DOI 10.1007/s12290-016-0384-8

ARTICLE

Digital foreign policy: how digital tools can further Europe's foreign policy goals

Łukasz Antoni Król

Published online: 11 April 2016

Abstract The security threats Europe is now facing, such as hybrid warfare, propaganda campaigns and information warfare, frequently include a digital dimension. At the same time, digital tools offer an immense potential for change in the European neighbourhood, not least in their ability to equip and inspire pro-democracy protesters, particularly those facing a repressive security apparatus. Digital policy cannot therefore become an afterthought but needs to be deeply integrated into Europe's foreign policy and diplomatic efforts. Furthermore, the US's long-held Internet hegemony is beginning to fade, placing the EU in a good position to lead global Internet governance initiatives and ensure that they develop along open and liberal lines.

Keywords EU neighbourhood policy | Cybersecurity | Hybrid warfare | Internet | Governance | Democratisation | Internet freedom

This article was written while the author was employed in the Brussels office of Jacek Saryusz-Wolski, Member of the European Parliament and Vice-Chair of the European People's Party.

Ł. A. Król (✉)
Wilfried Martens Centre for European Studies, Rue du Commerce 20, 1000 Brussels, Belgium
e-mail: lukasakrol@gmail.com

Introduction

The battle for an open Internet is not merely a matter of political principle. It is also a means of achieving certain EU foreign policy goals, such as supporting democracy or combating hybrid war. Increased engagement in Internet policy would also allow the EU to boost its visibility in global foreign policy, humanitarian and democracy promotion programmes. This article will look into digital and foreign policy issues in the current geopolitical atmosphere, in which hybrid threats present new strategic difficulties. The first section describes the impact of the Internet on human rights defenders and civil society activists, including those who are pressing for greater transparency in Russia. The second section deals with cybersecurity. It covers cyber-attacks, which are becoming an important tool in hybrid warfare, and investigates ways of responding to them. The third section looks at current debates over the Internet's governance structures and analyses how the EU should engage in such discussions. The final section of the article explains how the EU could become a leading global player in digital foreign policy.

Digital diplomacy, or the way in which politicians and foreign ministries alike are increasingly turning to tools such as Twitter to manage aspects of their public communication, is quickly rising in importance. Yet an EU-wide digital diplomacy strategy could cause more harm than good by hampering the spread of the individual tones, attitudes and personalities that have enabled political Tweets to become such an important communication tool. While digital diplomacy could become an important tool in democratisation efforts and the fight against Russian propaganda, a deeper analysis therein lies in the realm of digital communications and marketing studies rather than foreign policy analysis, and is outside the scope of this paper.

The Internet, communications and human rights

Online connections play an overwhelmingly influential role during protests such as the Arab Spring. Protesters and activists themselves acknowledge the importance of social networks, while authoritarian governments' rapid reactions and threats to shut down Internet connections also suggest that they feel threatened by large-scale online mobilisation (Tkacheva et al. 2013). In a world in which authoritarian states frequently attempt to curtail free speech and control the media, the Internet can become a crucial sphere of resistance. In the Middle East, political and economic grievances certainly provided the backdrop for the Arab Spring demonstrations, but countless citizens also used online tools to organise their efforts, mobilise protests and hold authorities to account. Similarly, in Russia, a civil society created online helps to monitor elections, communicate with citizens and counter certain government narratives (Howard and Hussain 2013). Platforms such as blogs and social media are often able to present a contrarian message and have become a space for alternative opinions, something that is crucial in states that lack a free and independent media environment. An influential civil society vanguard can often organise itself online (Tkacheva et al. 2013) and create

an atmosphere of opposition that can spread to other social sectors, even in states with low Internet penetration.

The Internet's political impact in the EU's southern neighbourhood has been extensively studied by scholars, somewhat to the detriment of its impact among Europe's eastern neighbours. Yet Europe's eastern neighbours, as well as some of its member states, are feeling the impact of a hybrid warfare campaign that also has an informational dimension, necessitating an effective digital foreign policy response. In the past, Radio Free Europe and Radio Liberty effectively tackled the Soviet message because they not only broadcast Western views, but also interviewed civil society leaders in the Soviet sphere (Howard and Hussain 2013). Similarly, promoting active discussions online and aiding political activists in Russia would contribute towards an organic alternative public sphere that could weaken the Kremlin's propaganda grip and information monopoly within Russia and the surrounding regions. At the same time, media environments are not always fully mature, especially in authoritarian, developing or post-Soviet states, and many major publishers are often reluctant to disseminate politically sensitive content. The EU should therefore consider supporting independent publishers, news outlets or online platforms on which activists could post freely.[1] Such support could come in the form of technological help, since many activists do not have sufficient technical knowledge, or simply in the shape of funding for independent and investigative journalism.

With the notable exception of China,[2] most states find it difficult to eliminate politically troublesome content online. They prefer cracking down on those who author this content over pre-emptively preventing its spread.[3] Governments nonetheless have the upper hand in terms of digital resources and can wield control over the Internet's physical infrastructure, while civil society representatives often require outside assistance, such as media or cybersecurity training. While the Internet's low barriers to entry make it easy to create political blogs or platforms, activists also need to be wary and sufficiently well trained so as not to become easy targets of state repression (Morozov 2012). During the Arab Spring uprisings, as governments began to restrict Internet connections, a 'speak to Tweet' system developed by Google and Twitter helped protesters and dissidents to express themselves. It provided them with a phone number so that they could dictate messages which would be turned into Twitter posts. Similarly, tools such as The Onion Router (Tor), which anonymises online connections and was partially developed and funded by the US government, are also frequently employed by activists. Finally, many opposition figures would benefit immensely from better encryption services, which could help them to evade government surveillance.

[1] I am grateful to Ms Kateryna Kruk and Jacek Saryusz-Wolski, MEP, for helping me to better understand this concept.

[2] While much of China's online censorship is ruthlessly effective, some users have still been able to overcome it to some degree through the use of coded phrases. For more information see Qiang and Lyden (2013).

[3] Some states, notably Russia, are trying to implement real name policies and similar tools that would further restrict citizens' ability and readiness to post subversive content. Such plans, however, are still in their infancy and it remains to be seen what impact they will have.

In the digital era, technology can empower activists and authoritarians alike, and the EU should ensure that the former benefit the most from it. This could be achieved through providing tools and trainings that cover topics such as encryption, anonymous browsing, and overcoming government bans and blockades of websites. European institutions should therefore look into measures such as spreading anonymisation software and training activists in digital skills and cybersecurity. These activities should be framed as both democratisation assistance and countermeasures against Russian propaganda. Politicians must resist the temptation to blame encryption and threaten to restrict it in the wake of successful terrorist attacks. Criminals and terror groups will always find ways of using or smuggling effective encryption products (Doctorow 2015), while any ban on secure communications will cause the most harm to human rights activists and non-governmental organisations (NGOs) that need to relay anonymous messages in repressive environments. Finally, the EU should strengthen its export ban on surveillance technologies (Pop 2011), as many European companies continue to create products used for authoritarian surveillance.

Cybersecurity, hybrid warfare and traditional security actors

Information warfare aims to influence hearts and minds rather than directly steal data, cause physical harm or damage infrastructure. The latter effects, however, can be accomplished using cyber-attacks, a broad term that encompasses several dimensions and potential types of attack, including theft, espionage and cyberwar:

- Cybercrime, frequently theft and fraud, not only causes immense economic losses (estimated at around $400 billion in 2014) (McAfee 2014) but, like maritime piracy, is a cross-border phenomenon and therefore also a foreign policy matter.
- Cyber-espionage involves the theft of intellectual property from governments and companies.
- Cyberwarfare refers to large-scale actions against the state, and could be directed against infrastructure (including energy networks), state services and similar targets.

Cybersecurity challenges traditional security paradigms in two ways. First of all, it is difficult to attribute a cyber-attack to a specific actor. Scholars have debated whether a politically motivated cyber-attack on Estonian government services was the work of an agitated Russian crowd who opposed a perceived anti-Soviet gesture by Tallinn or a state-sponsored response. This difficulty in attribution makes cyber-attacks a valuable component of hybrid warfare. Immediately before Russia's 2008 invasion of Georgia, Tbilisi's government servers were flooded with significant amounts of data, knocking them offline. The timing and circumstantial evidence suggest that Moscow was responsible, but proving such a claim with complete certainty is almost impossible. The EU should take steps to tackle the cross-border nature of cybercrime and could, through

bilateral treaties, make cybercrimes illegal in both their country of origin and the country they target (as proposed by Nye 2014).

Second, cybersecurity requires deep public–private cooperation. The public sector often has the law enforcement and (in the case of cyberwarfare) military expertise to address cyber-incidents, while the private sector often owns and manages most of the infrastructure which could be hit by such attacks. It is therefore crucial that both sectors actively communicate, declare security breaches and trust one another. The EU should formulate a policy on how to respond to both private and state-sponsored cybercrime and cyberwarfare, while differentiating between them and ensuring that the reaction is balanced, proportionate and nuanced. This policy should be consistent across the EU, as data leaks or attacks on one state could spill over and have much wider repercussions.[4] Similarly, the reporting of breaches should be made mandatory. This would ensure that every organisation that has been broken into reveals details of the breach and cooperates with the relevant authorities to prevent future incidents.[5] Grouping all types of attack under the common umbrella term of 'cybersecurity' is often unhelpful, since different attacks are perpetrated by different actors and require different reactions. While a state's intelligence and military services should investigate and react to instances of cyberwarfare, such a reaction is counterproductive when dealing with cybercrime such as theft. The cyber-attacks against Sony that were attributed to North Korea were framed by the US government as an attack on American freedoms of speech (Kerry 2014). Such a response, however, did not resolve the issue faster and unnecessarily blurred the line between international law enforcement and military affairs. States should distinguish between different types of cybersecurity problems and create differentiated, nuanced approaches.

Cyberwarfare and the military dimension of cybercrime

The current war in Eastern Ukraine has witnessed the use of some low-level cyber-tactics (Geers 2015; Coyle 2015), which will probably become more prominent in future hybrid warfare scenarios. Such tactics can be used in conjunction with propaganda campaigns to shape narratives, for example by knocking opposition websites offline and blurring the line between information warfare and direct attacks on physical infrastructure. Furthermore, it is very difficult to tell whether such actions are perpetrated by a state, private individuals or non-state groups. Finally, cyber-attacks are easy to conduct but difficult to defend against.

[4] These ideas were first put forward at a workshop entitled 'Cybersecurity and Advanced Threats in Practice' that took place at the European Parliament on 24 March 2015, led by Jason Steer from computer security firm FireEye.

[5] See Footnote 4.

As the cases of Georgia, Estonia and Ukraine demonstrate, all states, especially the most vulnerable ones, must improve their cyber-defences and resilience. Since such defences often concern civilian infrastructure, civilian EU assistance could also be used to bolster them. However, it is possible to alleviate the worst consequences of such attacks. Shortly after the 2008 attack, Georgian government websites were successfully transferred to less vulnerable US servers (Korns and Kastenberg 2009). The EU could encourage member states to engage in a similar type of burden sharing. During a potential future cyber-attack, member states could host attacked states' websites and information, which could significantly reduce an aggressor's ability to disrupt digital communications during hybrid campaigns.

A cyber-attack has an immense offensive balance. Unlike a traditional attack, the cost of carrying out a cyber-attack is very low while the cost of defending a state or organisation against one is very high. This also means that states are constantly trying to find new ways of deterring cyber-attacks, the most notable of which is NATO's Tallinn Manual (Schmitt 2013). It argues, among other things, that cyber-attacks count as a 'use of force'; that they can be classified as 'armed attacks'; and that some cyber-attacks should be met with a military, rather than merely a law enforcement, response. The Tallinn Manual, however, is not official NATO policy and has not been codified into any treaties. The EU should think deeply about the ways in which cyber-tactics form part of hybrid warfare and how to respond to them. Just as the recent invasion of Eastern Ukraine raised questions over what role NATO's Chapter Five would play if a member of the Alliance was invaded by troops not operating under a national flag in a hybrid warfare scenario, so similar issues should be discussed with regard to cyber-attacks. The EU should look into the ethics and norms of cyberwarfare and help to form treaties that define legitimate and illegitimate targets. The European External Action Service is currently working on defining international norms that ban powers from targeting each other's critical civilian infrastructure, and the other EU institutions should support such efforts.

Global Internet governance

While the Internet's current structures often help activists, promote free exchange of information and aid democracy, such benefits are not inevitable. Designing the Internet's wider governance mechanisms is rapidly becoming a foreign policy prerogative, since many of the Internet's political and economic benefits rely on its open nature, which is increasingly under threat.

The economic and political benefits of the Internet are so immense that many authoritarian states have also embraced it. While some, such as North Korea, have managed to cut almost all of their citizens off from the Internet, they are the exception rather than the rule. Despite this, many authoritarian and developing states are trying to assume greater domestic control of the Internet.

EU and OECD states, in contrast, tend to promote the status quo, in which the Internet is governed by many different organisations through a system of consensus. Technical standards are mostly determined by groups of engineers. Many politicians, think tanks (Negroponte et al. 2013) and the European Commission (2015) have spoken out in favour of this multi-stakeholder, which has several advantages:

- It effectively replicates the design of the Internet. The idea of absolute state control clashes with the nature of universal transnational networks.
- It enables further organic growth. The Internet is expanding very quickly, making soft regulations much more effective than hard laws.
- It preserves human rights and free discussion online which could be at threat otherwise. A system in which states have greater control over the shape of their regional networks, as promoted by Russia and China, could lead to entire regions being closed off from the global Internet, an end to online anonymity or increased censorship.
- It allows for an effective response to many cybersecurity issues. As German representatives (Schaller and Thimm 2014) and analysts such as former US Deputy Secretary of State John Negroponte argue, cybersecurity is best maintained through an open Internet and common agreements on how to tackle cybercrime and cyber-attacks. Furthermore, since cybercrime spans both the public and private spheres, a joint public and private governance model for the Internet, rather than a merely state-driven one, is better placed to fight it (Negroponte et al. 2013).

Discussions over Internet governance are moving into the realm of high politics (Raymond and Smith 2013), and many states have begun to challenge the multi-stakeholder model (DeNardis and Raymond 2013). Some, including Russia and China, are trying to assert a greater degree of sovereignty over the Internet. Others, mostly OECD states, are still actively promoting the multi-stakeholder model. Finally, many post-colonial states are undecided but tend to support the sovereignty-driven approach as they feel that the current order is too US-centric and does not adequately represent their interests

Many of the discussions about the future of the Internet and its governance are therefore also proxy debates about the wider role of the West in global governance. This debate comes at an important time. Supporters of the Transatlantic Trade and Investment Partnership argue that the agreement will help the EU and the US to shape new global economic norms. Similarly, the EU and the US also have important opportunities to address global Internet governance through other trade deals and diplomatic actions.

The flaws of the current Internet governance structures need to be addressed. The EU should engage with other powers, particularly those in the developing world, and assure them that the current system represents their interests. However, as it stands the current governance system is still too US-centric. A further problem is that the multi-stakeholder model will lead to the emergence of too many decision-making bodies. Wealthier states, which can afford more technical and diplomatic resources, are therefore better represented and tend to have a louder voice within such organisations (Negroponte

et al. 2013). Similarly, larger companies have much greater resources and are therefore disproportionately well represented and more influential than smaller firms and NGOs. This is a key concern of developing states and small civil rights and consumer groups, and needs to be addressed. Despite those flaws, the multi-stakeholder model is the most effective method of Internet governance and the EU should continue to promote it and oppose a sovereign, state-driven Internet. This could be achieved through leading by example and ensuring that member states embrace open Internet norms, promoting the multi-stakeholder model within international organisations, and perhaps by including provisions for an open Internet in some aid and bilateral trade deals.

Global digital democracy programmes and the EU

Several groups already carry out digital foreign policy programmes, the most prominent being the US's Internet Freedom programme, run by the Department of State. The programme encompasses several aspects of digital foreign policy, including efforts to create and distribute censorship circumvention and anonymisation technologies, to begin a dialogue with US firms about the export of surveillance software and to advocate for an open Internet based on the multi-stakeholder model (Clinton 2010; Henry et al. 2014). RAND Corporation conducted a large-scale analysis of the programme and concluded that it was highly effective, particularly its backing of anonymisation software Tor, which was used in over half of the projects it pursued (Henry et al. 2014). However, the effectiveness of the Internet Freedom programme has not been sufficiently analysed by academics and practitioners, and it remains an open question whether it could provide an effective template for an EU digital foreign policy.

Even though digital foreign policy programmes already exist and both governments and some private companies such as Google (through Jigsaw, formerly known as Google Ideas) and Facebook (through Internet.org) try to promote free expression online, there are still many ways in which the EU could add significant value. Schemes such as the Freedom Online Coalition, a group of states campaigning for a multi-stakeholder Internet, provide an important platform for dialogue. Such conversations, however, are unlikely to bring about significant results if they are not tied to the atmosphere of urgency and momentum usually associated with democratisation and foreign policy projects.

The EU, however, could tie digital foreign policy programmes into certain aspects of the European Neighbourhood Policy, which already has significant influence in the region it covers. It could use institutions such as trade agreements or accession negotiations to promote an open Internet built along multi-stakeholder lines and greater government tolerance towards online anonymity. Not all Neighbourhood partners were rated as 'free on the Net' in the annual Freedom House ranking (Kelly et al. 2015). Much could be done to improve their standing. The EU could also make greater use of its networks, especially within the Eastern Partnership. It is not enough that tools such

as anonymisation software exist. They also need to target the right people, and the EU could use its links with civil society, activists and non-profit organisations to accomplish this.

Finally, while some states have implicitly accepted the US as the online hegemon that sets most Internet standards and leads on Internet freedom issues, the revelations of the US National Security Agency's spying activities have caused significant damage to its soft power in that regard. The RAND Corporation report (Henry et al. 2014) investigating the efficacy of American Internet Freedom policies acknowledges that many pro-democracy activists will not want to be affiliated with the US or use digital tools produced by its government. The EU's soft power has a different reach and orientation to that of the US, and its digital foreign policy tools and advocacy could therefore reach states and activists that view the Atlantic hegemon with ambivalence or distrust.

Any state or multinational actor engaging in digital foreign policy will face significant challenges. Political crises and demonstrations unfold quickly. It can be very difficult to immediately identify groups that need digital advice and anonymisation tools. Similarly, political actors are not experts at creating technological tools (Henry et al. 2014) and will require the close cooperation of technology firms and NGOs. Finally, policymakers will need to avoid the temptation of seeing the Internet solely as a force for democracy and liberation (Morozov 2012). The web will not organically reject attempts at authoritarian control, propaganda and surveillance. The EU should find ways of actively subverting and resisting such efforts.

Conclusion

Some aspects of foreign policy and democracy support are moving into the digital realm: human rights defenders and activists often use the Internet as a powerful tool, cybercrime and cyber-attacks cross borders, and the global nature of the Internet requires international collaboration. The EU has the potential to lead on matters of digital foreign policy. It has an advanced technology industry, a history of promoting human rights, the necessary financial capabilities and soft power. Furthermore, many states are becoming increasingly frustrated with what they perceive to be US dominance in digital policy and issues. Europe has the potential to emerge as a new leader in this area—as a region that can continue the previously US-led campaign for an open and democratic Internet, but is not weighed down by a legacy of years of excessive online control.

Just as with other policy areas, the EU needs to look into both short- and long-term actions when dealing with digital foreign policy. In the short term, it is crucial to protect pro-democracy activists and to find new ways of tackling hybrid war and reacting to new security threats. However, there is also a real risk that other states will begin to close off or censor their Internet connections, negating many of the potential short-term gains of an effective digital foreign policy. Short-term action should therefore be complemented by an effective long-term strategy to further engage in Internet governance forums and promote an open Internet based on liberal principles.

References

Clinton, H. (2010). Remarks on Internet freedom. US Department of State, 21 January. http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm. Accessed 30 September 2015.

Coyle, J. J. (2015). Russia has complete informational dominance in Ukraine. Atlantic Council, 12 May. http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-has-complete-informational-dominance-in-ukraine. Accessed 1 November 2015.

DeNardis, D. L., & Raymond, M. (2013). Thinking clearly about multistakeholder Internet governance. *SSRN Electronic Journal*. doi:10.2139/ssrn.2354377.

Doctorow, C. (2015). Encryption won't work if it has a back door only the 'good guys' have keys to. *The Guardian*, 1 May. http://www.theguardian.com/technology/2015/may/01/encryption-wont-work-if-it-has-a-back-door-only-the-good-guys-have-keys-to. Accessed 21 November 2015.

European Commission. (2015). The sustainability of the multistakeholder model. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=5648. Accessed 29 February 2016.

Geers, K. (ed.). (2015). *Cyber war in perspective: Russian aggression against Ukraine*. Tallinn: NATO CCD COE Publications.

Henry, R., Pettyjohn, S., & York, E. (2014). *Portfolio assessment of Department of State Internet Freedom program: An annotated briefing*. RAND Corporation Working Paper, February. http://www.rand.org/pubs/working_papers/WR1035.html. Accessed 1 November 2015.

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave?: Digital media and the Arab Spring*. Oxford Studies in Digital Politics. Oxford, New York: Oxford University Press.

Kelly, S., Earp, M., Shahbaz, A., Truong, M., Reed, L., & Ellerbeck, A. (2015). Freedom on the Net 2015. https://freedomhouse.org/report/freedom-net/freedom-net-2015. Accessed 7 March 2016.

Kerry, J. (2014). Condemning cyber-attack by North Korea. US Department of State, 19 December. http://www.state.gov/secretary/remarks/2014/12/235444.htm. Accessed 3 January 2016.

Korns, S. W., & Kastenberg, J. E. (2009). *Georgia's cyber left hook*. US Army Strategic Studies Institute. http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/08winter/korns.pdf. Accessed 1 November 2015.

McAfee. (2014). *Net losses: Estimating the global cost of cybercrime*. Center for Strategic and International Studies, June. http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf. Accessed 12 November 2015.

Morozov, E. (2012). *The Net delusion: How not to liberate the world*. London: Penguin.

Negroponte, J. D., Palmisano, S. J., & Segal, A. (2013). *Defending an open, global, secure, and resilient Internet*. Council on Foreign Relations, Independent Task Force Report no. 70. http://i.cfr.org/content/publications/attachments/TFR70_cyber_policy.pdf.pdf. Accessed 6 January 2016.

Nye, J. S., Jr. (2014). *The regime complex for managing global cyber activities*. Centre for International Governance Innovation and The Royal Institute for International Affairs, Paper Series 1, May. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf. Accessed 12 January 2016.

Pop, V. (2011). EU companies banned from selling spyware to repressive regimes. *EU Observer*, 11 October. https://euobserver.com/cyber/113791. Accessed 5 January 2016.

Qiang, X., & Lyden, J. (2013). In China, avoiding the 'Great Firewall' Internet censors. *NPR.org*, 7 September. http://www.npr.org/templates/story/story.php?storyId=220106496. Accessed 11 January 2016.

Raymond, M., & Smith, G. (2013). *Reimagining the Internet: The need for a high-level strategic vision for Internet governance*. Centre for International Governance Innovation, Internet Governance Paper no. 1. https://www.cigionline.org/sites/default/files/no1_7.pdf. Accessed 29 February 2016.

Schaller, C., & Thimm, J. (2014). Internet governance and the ITU: Maintaining the multistakeholder approach. The German perspective. Council on Foreign Relations, 22 October. http://www.cfr.org/internet-policy/internet-governance-itu-maintaining-multi-stakeholder-approach/p33654. Accessed 24 October 2015.

Schmitt, M. N. (ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge; New York: Cambridge University Press.

Tkacheva, O., Schwartz, L. H., Libicki, M. C., Taylor, J. E., Martini, J., & Baxter, C. (2013). *Internet freedom and political space*. Santa Monica, CA: RAND National Research Defense Institute.

Łukasz Antoni Król *is a political scientist and independent researcher studying the links between the Internet, democracy and nation-building. He is a graduate of the Universities of St Andrews and Cambridge.*